Daily Open Source Infrastructure Report
4 May 2012

Top Stories

- The number of illnesses linked to the outbreak of Salmonella infection likely caused by raw tuna sushi has grown to 258 in 24 states and Washington D.C., federal officials reported. – *Food Safety News* (See item **18**)
- Two farms were quarantined by the U.S. Department of Agriculture as the agency continued to investigate the discovery of mad cow disease at a California dairy farm. – *CNN* (See item **19**)
- Miami-Dade County's 7,500 miles of sewage lines are in such decrepit shape and rupture so frequently, federal environmental regulators are demanding repairs and upgrades that could cost upwards of $1 billion. – *Miami Herald* (See item **25**)
- A strike force of agents and investigators, led by the Departments of Justice and Health and Human Services, charged 107 persons in 7 cities with Medicare fraud involving more than $452 million in false billings. – *Washington Times* (See items **30**, **36**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *May 3, Pennsylvania Reading Eagle* – (Pennsylvania) **Copper thieves damage substations.** Met-Ed and police in Pennsylvania were investigating a series of thefts of copper grounding wires and equipment from electric substations. The thefts occurred in West Reading, Muhlenberg Township, Lincoln Park, Leesport, and the Moselem Springs area of Richmond Township, a Met-Ed spokesman said. People climbed safety fences or cut through the fences and damaged the substations, making them unsafe for employees who routinely service the facilities and must repair the damage. "The damage also has resulted in power outages to homes and businesses as recently as [the week of April 23]," he said. The spokesman urged the public to report any suspicious activity.
   Source: http://readingeagle.com/article.aspx?id=383853

2. *May 2, Associated Press* – (Wyoming) **Wyo. mine blast picked up on seismographs.** An explosion at a coal mine near Gillette, Wyoming was big enough to register on seismographs on the scale of a small earthquake, the Associated Press reported May 2. Some people in Gillette reported feeling the ground shake from 16 miles away. The blast registered as large as a magnitude 4.5 earthquake but had the signature of a human-caused explosion. The Associated Press reported using explosives is a routine part of removing dirt and soil at the coal mines where the blast occurred. The explosion happened in the area of Cloud Peak Energy's Cordero Rojo mine. Mine explosions that register with such force are rare. Sheriff's officials said they had not heard of any emergency at the mines.
   Source: http://k2radio.com/wyo-mine-blast-picked-up-on-seismographs/

3. *May 2, Associated Press* – (Texas) **Official: No risk of spill after tanker accident.** A port official said there was no threat of an oil spill after a 750-foot tanker collided with a floating rig off the Texas Gulf Coast, tearing a hole in the ship's bow. The Port of Corpus Christi operations director said the ship called the "FR8 Pride" was inbound with a load of fuel oil May 2 when it lost power and veered into a rig being positioned by tugboats to enter the Corpus Christi ship channel. There were no injuries and there was no threat of pollution from the accident. The ship was anchored in the Gulf of Mexico after the accident about 3 miles off of Port Aransas.
   Source: http://www.businessweek.com/ap/2012-05/D9UGOKVO2.htm

For more stories, see items **13**, **15**, **23**, **47**, and **51**

[Return to top]

Chemical Industry Sector

4. *May 3, KYW 3 Philadelphia* – (Pennsylvania) **Trucks carrying chemicals banned from Platt Bridge until 2014.** Tractor trailer rigs and tanker trucks carrying chemicals or other hazardous materials will be banned from the Platt Bridge in southwest Philadelphia beginning May 7. A Pennsylvania Department of Transportation official said the ban will be in effect for 2 years, until the summer of 2014, when reconstruction work on the bridge -– which carries Route 291 over the Schuylkill River -– is expected to be finished. He said traffic is now restricted to one lane in each direction with motorists directed into concrete "cattle chutes" to keep them away from construction crews. He said safety concerns resulted in the truck ban. "The police department and fire department are very concerned about any incident that would occur on the bridge involving a large truck or would involve any type of hazardous materials spill." The official said the big issue is emergency crews even being able to get to a serious accident scene.
   Source: http://philadelphia.cbslocal.com/2012/05/03/trucks-carrying-chemicals-banned-from-platt-bridge-until-2014/

For another story, see item **28**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

See item **35**

[Return to top]

Banking and Finance Sector

5. *May 3, IDG News Service* – (International) **Hackers blackmail Belgian bank with threats to publish customer data.** Hackers claimed to breach the systems of the Belgian credit provider Elantis and threatened to publish confidential customer information if the bank did not pay $197,000 before May 4, according to a statement

posted to Pastebin May 1. Elantis confirmed the data breach May 3, but the bank said it would not give in to extortion threats. The hackers claimed to capture log-in credentials and tables with online loan applications that hold data such as full names, job descriptions, contact information, ID card numbers, and income figures. According to the hackers, the data was stored unprotected and unencrypted on the servers. To prove the hack, parts of what the hackers claimed to be captured customer data were published. The hackers contacted the bank via e-mail April 27, said a spokeswoman for Belfius Bank, Elantis' parent company. "We assume they possibly captured the data of 3,700 customers," she said, adding that the compromised data could belong to existing and potential customers. Elantis customers were informed of the data breach, according to the spokeswoman. After finding out what happened, the Elantis site was taken offline and the bank contacted the Belgian Federal High Tech Crime Unit, which is now investigating the case, she said. An unnamed specialized American security firm is also conducting an investigation, she added.
Source:
http://www.pcworld.com/businesscenter/article/254908/hackers_blackmail_belgian_bank_with_threats_to_publish_customer_data.html

6. *May 3, Associated Press* – (Virginia) **FBI, police investigate bank robberies.** The FBI said four recent bank robberies in Sussex and Chesterfield counties in Virginia appear to have been committed by the same suspects. The first robbery occurred March 27 at the Bank of Southside Virginia in Jarratt. It was followed by robberies at the Central Virginia Bank in Midlothian April 3, the BB&T in Wakefield April 19, and the Bank of Southside Virginia in Stony Creek April 23. One armed man held up the first two banks. Two armed men robbed the other banks. The robberies are being investigated by the FBI, the Sussex County Sheriff's Office, and the Chesterfield County Police Department.
Source: http://www.wavy.com/dpp/news/virginia/fbi-police-investigate-bank-robberies

7. *May 2, San Gabriel Valley Newspapers* – (California) **Whittier parolee accused of being 'Stretch Bandit' bank robber.** Prosecutors charged a Whittier, California parolee who the FBI knows as the "Stretch Bandit" with five San Gabriel Valley bank robberies following his arrest in April at the end of a police chase, San Gabriel Valley Newspapers reported May 2. He was charged with five counts of second-degree robbery, as well as one count of evading police, Los Angeles County district attorney's officials said in a written statement. "[He] is suspected of robbing a U.S. Bank in Hacienda Heights on July 6, 2011; a Bank of the West in Rowland Heights on July 12, 2011, and again on Jan[uary] 11, 2012; a Citibank in Rowland Heights on Jan[uary] 14; and the First Federal Credit Union in West Covina on April 23," a district attorney's office spokeswoman said. He was arrested April 23, just after the West Covina bank robbery, West Covina Police officials said at the time. After robbing the bank, the suspect led officials on a chase in a white van, a West Covina Police lieutenant said the day of the arrest.
Source: http://www.pasadenastarnews.com/ci_20533458/whittier-parolee-accused-being-stretch-bandit-bank-robber

8. *May 2, ATM Marketplace* – (National; International) **Crooks in 8 countries tap NZ bank accounts with skimmed ATM card data.** Using counterfeit cards striped with data skimmed from New Zealand bankcard holders, thieves withdrew cash at ATMs in the Dominican Republic, Bulgaria, Croatia, Italy, the Netherlands, Thailand, the United States, and South Africa, ATM Marketplace reported May 2. The New Zealand Herald said detectives were still searching for two men who entered the country earlier in 2012 and used skimmers at ANZ and National Bank ATMs in four cities to steal card information. The scam, which was discovered in late March, ultimately affected 500 customers of the 2 banks. All customers were reimbursed for their losses, which totaled $812,400. Police in Auckland, New Zealand, identified two men caught on security cameras whom they believe installed the skimmers. However, they told the New Zealand Herald the two most likely left the country before their scam was discovered.
Source: http://www.atmmarketplace.com/article/193901/Crooks-in-8-countries-tap-NZ-bank-accounts-with-skimmed-ATM-card-data

9. *May 2, Associated Press* – (National; International) **UK arrests 7 on suspicion of funding terror.** Seven people were arrested in Great Britain on suspicion of financing terrorism in Somalia by smuggling a leaf that can produce a mild high into the United States, officials said May 1. Scotland Yard said the group was arrested as part of an operation that involved Homeland Security Investigations, the investigative branch of U.S. Immigrations and Customs Enforcement (ICE). It investigated a network suspected of illegally exporting a leaf known as khat from the United Kingdom, where it is legal, to the United States and Canada, where it is a controlled substance, Scotland Yard said. "The proceeds generated by this illegal activity (were) then transferred back to Somalia," a spokesman for ICE said. He added that the khat mostly originated from Kenya, and U.S. law enforcement officials were working closely with their counterparts overseas on the investigation. British police said one woman and six men were arrested May 1 at four separate residences in London, Coventry, and Cardiff, Wales. Those four homes are being searched along with seven other residential addresses and a business address in Coventry, police added. Police said the seven people arrested are suspected of involvement in funding a terrorist organization and laundering the proceeds of crime for that purpose.
Source: http://www.google.com/hostednews/ap/article/ALeqM5iSKIv2aF2FA-IHAaZKwvbATi9TRQ?docId=af3bf8ee287e4036aed4e593ddf8f2ec

10. *May 1, U.S. Federal Trade Commission* – (National) **FTC wins court judgment against massive get-rich-quick infomercial scam.** The U.S. Federal Trade Commission (FTC) won a court judgment against the marketers of three get-rich-quick systems who deceived nearly a million consumers, according to a May 1 press release. The FTC is seeking more than $450 million in monetary relief. A district judge in California granted the FTC's request for summary judgment April 20 and asked the agency and defendants to submit arguments on the appropriate remedy. The marketers are behind the infomercials for the "Free & Clear Real Estate System," "Real Estate Riches in 14 Days," and "Shortcuts to Internet Millions." The court found the infomercials misled consumers in violation of the FTC Act, and despite the marketers' easy-money claims for the systems, which cost $39.95 each, nearly all consumers who bought them lost money. Regarding the Free & Clear Real Estate System, the court

found the defendants falsely said consumers could purchase homes at tax sales in their own area for pennies on the dollar and they could make money easily with little financial investment. The court found the earnings claims in the Real Estate Riches in 14 Days infomercial were false, and the Shortcuts to Internet Millions infomercial misled consumers. In contrast to the infomercials' claims, the court found that less than 1 percent of consumers who purchased the systems made any profit whatsoever. In addition, the defendants offered personal coaching services, which cost up to $14,995, to consumers who purchased any of the three systems. The court found that almost all consumers who purchased coaching programs lost money.
Source: http://www.ftc.gov/opa/2012/05/johnbeck.shtm

For another story, see item **30**

[Return to top]

Transportation Sector

11. *May 3, Martinsburg Journal* – (West Virginia) **Man dies in school bus accident.** A Virginia man died May 3 when his vehicle crossed the median of Interstate 81 and collided with a Berkeley County school bus occupied by 37 students near Martinsburg, West Virginia. Of the 37 students aboard the bus, 31 were checked out and evaluated by emergency medical services personnel at the scene and were transported to school, while another six students were transported by ambulance to a hospital. Five students later were transported throughout the day to the emergency department by parents who wanted their children evaluated, a hospital spokesperson said. By the afternoon, all 11 students had been treated and released.
Source: http://www.journal-news.net/page/content.detail/id/579004/Man-dies-in-school-bus-accident.html?nav=5006

12. *May 3, Indianapolis Star* – (Wisconsin; Indiana) **Ex-Frontier employee faces charges of making threats.** Federal charges were filed against a former employee of Frontier Airlines, alleging he sent a letter threatening to kill executives of the airline's Indianapolis-based parent company, Republic Airways Holdings, the Indianapolis Star reported May 3. The letter threatened to harm other employees and to blow up airplanes, authorities said. The man, who was laid off in April from his job with Frontier in Milwaukee, was arrested and eventually apologized for his actions, saying he intended no harm, court filings showed. The charges, based on an FBI investigation, were filed in U.S. District Court for the Eastern District of Wisconsin, where a preliminary hearing was scheduled for May 4.
Source: http://www.indystar.com/article/20120503/BUSINESS/205030337/Ex-Frontier-employee-faces-charges-making-threats

13. *May 3, Jacksonville Times-Union* – (Florida) **Bomb squad safely removes 'suspicious device' from CSX tracks near Jacksonville power plant.** The Jacksonville Sheriff's Office bomb squad safely removed what police described as a "suspicious device" deliberately placed under the rails of CSX tracks in Jacksonville, Florida, the Jacksonville Times-Union reported May 3. The device was removed about 3 hours after

it was discovered by a CSX Transportation Police Department special agent on routine patrol, said a company spokesman. Police would not describe the device, and they did not say whether it was capable of exploding. The FBI confiscated the device. No injuries occurred, and no evacuations were ordered, but firefighters remained on the scene in case they were needed. Authorities handled the discovery of the device with extra care because it was near critical infrastructure, including a JEA power plant. About 10 to 12 freight trains travel the track daily.
Source: http://jacksonville.com/news/crime/2012-05-02/story/bomb-squad-safely-removes-suspicious-device-csx-tracks-near-jacksonville#ixzz1toFwaLtQ

14. *May 3, MSNBC* – (California) **Hunt on for gunman in birdshot-firing spree in Carson, California.** The hunt was on near Carson, California, for a birdshot-firing gunman believed responsible for at least five shootings in about a week, the Los Angeles County Sheriff's Department said. The shotgun-toting suspect injured two people and damaged at least four cars between April 18 and April 26, MSNBC reported May 3. The shooting spree appears to have started when a woman walking along Main Street in Carson was struck in the arm. The other incidents involved motorists whose cars were struck by gunfire as they drove, two on city streets and two on nearby Interstate 110. One man was sent to a hospital for two days, NBCLosAngeles.com reported. In three cases, the birdshot struck vehicles without breaking glass or injuring people inside. No new leads were reported as of May 3.
Source: http://usnews.msnbc.msn.com/_news/2012/05/03/11522658-hunt-on-for-gunman-in-birdshot-firing-spree-in-carson-california?lite/

15. *May 3, Associated Press* – (Florida) **Fuel tanker overturns, I-75 south closed in SW Fla.** Deputies said fuel was leaking from an overturned tanker truck just south of Exit 161 on southbound Interstate 75 in Punta Gorda, Florida, May 3. Deputies said the driver escaped without injury. They said initial reports indicated the tanker was carrying 6,000 gallons of diesel fuel and 1,400 gallons of gasoline. It was not immediately known how long the interstate would be closed or how much fuel leaked from the tanker. Traffic heading south on Interstate 75 was being rerouted to U.S. 41.
Source: http://www.mysuncoast.com/news/state/story/Fuel-tanker-overturns-I-75-south-closed-in-SW-Fla/oWudMXzZG0q8TnMkuuGhTg.cspx

For more stories, see items **4**, **47**, and **51**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

16. *May 3, Food Safety News* – (Missouri) **Raw milk still suspect in 14 Missouri E. coli cases.** Fourteen cases of E. coli O157:H7 infection, including at least two severe cases requiring hospitalization, were confirmed in the central Missouri outbreak linked to unpasteurized milk, Food Safety News reported May 3. A raw milk dairy in Howard County was implicated as the source of the illnesses. A toddler from Boone County who was given raw milk developed symptoms of hemolytic uremic syndrome, a complication of E. coli infection that leads to kidney failure. The child remained hospitalized May 2. All 14 outbreak patients have similar lab results, geographic proximity, and/or case history, according to a spokeswoman for the state department of health and senior services. The week of April 23, the state identified the suspect Howard County dairy as Stroupe Farm, which halted the sale of its unpasteurized products.
Source: http://www.foodsafetynews.com/2012/05/missouri-says-14-e-coli-cases-may-be-from-raw-milk/

17. *May 3, Food Safety News* – (Maryland; Virginia; Washington, D.C.) **Recall expanded for sprouts with Listeria risk.** Henry's Farm Inc. of Woodford, Virginia, expanded the recall of its soybean sprouts to include natto soybean sprouts because they may be contaminated with Listeria monocytogenes, Food Safety News reported May 3. The initial recall was announced April 27. Test sampling by the State of Virginia's Food Safety and Security Program returned positive results for Listeria. The recalled sprouts were distributed to retail stores in Virginia, Maryland, and Washington, D.C. According to state authorities, the lack of coding or other traceback labeling information made it difficult to determine the quantity of sprouts distributed.
Source: http://www.foodsafetynews.com/2012/05/recall-expanded-for-sprouts-with-listeria-risk/

18. *May 3, Food Safety News* – (National) **Salmonella sushi outbreak cases jump to 258.** Three more states reported illnesses linked to the outbreak of Salmonella infection likely caused by raw sushi tuna imported from India, and the total number of confirmed cases rose to 258, the Centers for Disease Control and Prevention (CDC) reported May 2. The CDC's April 26 update on the Salmonella Bareilly and Salmonella Nchanga infections tied to the product called tuna scrape listed 200 cases from 21 states and Washington, D.C. California, Nebraska, and Tennessee have now reported outbreak-related cases. The 58 new cases include 13 reported by Pennsylvania, 8 by Illinois and New Jersey, 7 by Virginia, 6 by New York, 4 by Maryland, 3 by Massachusetts, 2 by California and Tennessee, and 1 each by Connecticut, Georgia, Nebraska, North Carolina, and Wisconsin. Eleven people infected with the outbreak strain of Salmonella Nchanga were reported from five states: five from New York, two from Georgia and New Jersey, and one from Virginia and Wisconsin. Nearly 59,000 pounds of the frozen yellowfish tuna scrape was recalled by the distributor, Moon Marine Corp. of Cupertino, California. Many of the people sickened reported eating "spicy tuna" sushi before they became ill.
Source: http://www.foodsafetynews.com/2012/05/salmonella-sushi-outbreak-cases-jump-to-258/

19. *May 3, CNN* – (California) **USDA quarantines 2 farms in mad cow investigation.** Two farms were quarantined by the U.S. Department of Agriculture (USDA) as the agency continued to investigate the April discovery of mad cow disease at a California dairy farm. Authorities launched an investigation at a calf ranch where the initial infected cow was raised 10 years ago, according to a statement released May 2 by the USDA. The week of April 23, the USDA documented the fourth confirmed U.S. case of Bovine Spongiform Encephalopathy (BSE) known commonly as mad cow disease, at a rendering facility in central California. USDA officials said the cow was never presented for human consumption and was not a threat. The farm where the cow was initially discovered has been under quarantine since the discovery, agriculture officials said. The May 2 announcement of a second quarantine involves a farm closely associated with the dairy where the sick cow was discovered, the USDA said. The agency is still trying to determine if any at-risk cattle are present at either of the farms. Source: http://www.cnn.com/2012/05/03/health/california-mad-cow/index.html?hpt=hp_t2

20. *May 2, Bloomberg* – (National) **Tainted beef sources to be tracked faster by investigators.** Sources of tainted beef will be identified faster under a U.S. plan to improve tracking of meat sent from suppliers and processors that may sicken consumers. Investigators will search for where the spoiled meat came from after their own tests find E. coli in beef rather than waiting days for multiple confirmation tests, the Agriculture Department (USDA) said May 2. The investigation to find the origin of contaminated product, such as a slaughterhouse or processor, will happen 24 to 48 hours faster, the USDA said. The plan would take effect in July after a 60-day public comment period. Establishments will have to prepare and maintain procedures for recalling meat and poultry and notify the agency within 24 hours if a product that could harm consumers has been shipped, a rule required under the 2008 Farm Bill. They will also have to document each re-evaluation of the systems they use to control pathogens in production. Identifying the source of bad meat means they can find out at slaughterhouses what conditions may have allowed E. coli to get into product, perhaps because the operation was not in compliance on those days or that the presence of a pathogen had been detected when the meat was on site, a food safety lawyer said. Source: http://www.businessweek.com/news/2012-05-02/tainted-beef-sources-to-be-tracked-faster-by-u-dot-s-dot-investigators

21. *May 2, WOWK 13 Huntington* – (West Virginia) **OSHA cites IHOP for South Charleston chlorine incident.** Federal regulators proposed $25,000 in civil penalties against IHOP Restaurants stemming from a chlorine incident at a West Virginia restaurant that sickened nine workers. The U.S. Occupational Safety and Health Administration said May 2 that it cited the company for five alleged serious safety and health violations at the South Charleston restaurant. They include failure to conduct a personal protective equipment hazard assessment and failure to provide training, eye protection, eye wash facilities, and material safety data sheets for chemicals used in the workplace. South Charleston fire officials said chlorine fumes dispersed throughout the building February 17 when workers mixed bleach and a cleaning agent together in a sink area.

Source: http://www.wowktv.com/story/18065526/osha-cites-ihop-for-wva-chlorine-incident

22. *May 2, Enid News and Eagle* – (Oklahoma) **Fire forces evacuation of ADM Milling workers.** ADM Milling workers were evacuated May 2 after a small fire broke out in the top of an elevator at the facility in Enid, Oklahoma. The fire started when a conveyor belt slipped, creating friction that caused a small smoldering fire, the Enid fire marshal said. Smoke came out of two windows on the top of the elevator. Firefighters used a 100-foot aerial ladder truck to get water to the fire, pouring water down the shaft and into the compartment where the fire was located. The truck's platform went up about 70 feet to tackle the fire. Firefighters fought the fire about 1 hour to ensure it was out, but they stayed on site to monitor the situation an extended period of time afterward. Several trucks answered the initial alarm.
Source: http://enidnews.com/localnews/x1378308228/Fire-forces-evacuation-of-ADM-Milling-workers

For more stories, see items **24** and **26**

[Return to top]

Water Sector

23. *May 3, WFTV 9 Orlando* – (Florida) **Bithlo residents mistakenly contaminate drinking water.** Hundreds of wells in Bithlo, Florida, will be tested throughout May after some residents mistakenly contaminated their drinking water with cancer-causing chemicals. The residents were trying to clean up their water because they live near an old gas station that leaked petroleum into the ground 25 years ago. Health officials said when the residents added chemicals to purify the water, they accidentally contaminated it. Of the 112 wells sampled, only 4 were found with contaminants, such as chloromethane and trihalomethane, from the oil spill. Two dozen wells that were not impacted were contaminated by residents.
Source: http://www.wftv.com/news/news/local/bithlo-residents-mistakenly-contaminated-drinking-/nNPyz/

24. *May 2, U.S. Environmental Protection Agency* – (Hawaii) **EPA fines three Big Island companies for failing to close cesspools.** The U.S. Environmental Protection Agency (EPA) resolved federal Safe Drinking Water Act cases against the Jazmin Family Trust, GLACS LLC, and Hula Daddy Kona Coffee with fines totaling $141,200 for failing to close their large capacity cesspools on the Big Island. The EPA's regional administrator for the Pacific Southwest said, "Over 2,800 large cesspools have been closed, but an alarming 1,200 are still in use. We are working to shut these illegal cesspools down." A large capacity cesspool discharges untreated sewage from multiple dwellings, or a non-residential location that serves 20 or more people per day. EPA regulations prohibited new large capacity cesspool construction after April 2000 and required closure of existing large cesspools as of April 2005.
Source:

http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/8269657b36c33632852579f20070a0e1!OpenDocument

25. *May 2, Miami Herald* – (Florida) **Feds file complaint, demand Miami-Dade County fix faulty sewer lines.** Miami-Dade County's 7,500 miles of sewage lines in Florida are in such decrepit shape and rupture so frequently, federal environmental regulators are demanding repairs and upgrades that could cost upwards of $1 billion. Authorities from the U.S. Environmental Protection Agency, the Department of Justice, and Florida Department of Environmental Protection met May 2 with local officials to begin negotiations. The director of Miami-Dade's Water and Sewer Department acknowledged the string of major ruptures in recent years, saying the aging network is "being held together by chewing gum." The potential $1 billion overhaul almost certainly means rate hikes for hundreds of thousands of residents who have historically paid some of the lowest fees in the state. The federal complaints were sketched out in a 78-page draft consent decree claiming Miami-Dade County has violated sections of the Clean Water Act, along with terms and conditions of its National Pollutant Discharge Elimination System permits. Miami-Dade has suffered at least three major sewer pipe breaks the past 3 years, and a recent internal report shows that 3 sections of 54-inch pipe under Biscayne Bay are so brittle they could rupture at any time. The director said a break in that pipe, which carries 25 million gallons of raw sewage each day from Surfside, Miami Beach, and Bal Harbour, could be "catastrophic." Engineers linked many of the worst breaks to defective pipe built by Interpace, a now-defunct company whose products were widely used in the 1970s. Now, some are failing decades earlier than expected because over time, steel reinforcement wires inside the concrete pipes have corroded, broken, and failed.
Source: http://www.miamiherald.com/2012/05/02/v-fullstory/2779936/feds-file-complaint-demand-miami.html

26. *May 2, WBBH 2 Fort Myers* – (Florida) **Low water levels in Cape canals prompt action.** Prior to recent rain, water levels in the canals of Cape Coral, Florida, were the lowest since the drought of 2007, WBBH 2 Fort Myers reported May 2. The Cape Coral Utilities director said the city was pumping drinking water into the irrigation water for the first time ever. "Our system is a pressurized system, so we want to maintain that to maintain adequate pressure for fighting fires and that is a concern," the director said. Members of the Cape Coral city council planned to vote on an ordinance to allow the city to enact a more stringent watering schedule when the canal levels get low. In the meantime, voluntary water restrictions were put in place.
Source: http://www.nbc-2.com/story/18065440/low-water-levels-in-cape-canals-prompt-action

27. *May 2, Olympic Peninsula Daily News* – (Washington) **Methane leak creates 'potentially explosive situation'.** A methane leak in Port Angeles, Washington's dormant landfill is creating "a potentially explosive situation," the public works and utilities director said May 2. Methane gas from the closed landfill is leaking into a cracked concrete stormwater pipe and out of the manhole. The pipe cracked because of natural settling of 3 to 4 feet in the past 6 to 7 years. Council members unanimously approved a $36,296 contract to repair the pipe, replacing the broken section with PVC

pipe as early as the week of May 7. The now closed landfill releases 220 cubic feet of methane gas and carbon dioxide per minute.
Source:
http://www.peninsuladailynews.com/article/20120503/news/305039988/methane-leak-creates-8216-potentially-explosive-situation-8217

28. *May 1, U.S. Environmental Protection Agency* – (National) **EPA to work with drinking water systems to monitor unregulated contaminants.** The U.S. Environmental Protection Agency (EPA) published a list of 28 chemicals and 2 viruses that approximately 6,000 public water systems will monitor from 2013 to 2015 as part of the agency's unregulated contaminant monitoring program, which collects data for contaminants suspected to be present in drinking water, but that do not have health-based standards set under the Safe Drinking Water Act (SDWA). The EPA will spend more than $20 million to support the monitoring. The data collected under the Unregulated Contaminant Monitoring Rule 3 (UCMR 3) will inform the agency about the frequency and levels at which these contaminants are found in drinking water systems across the United States and help determine whether additional protections are needed to ensure safe drinking water. State participation in the monitoring is voluntary. The EPA will fund small drinking water system costs for laboratory analyses, shipping, and quality control. The agency has standards for 91 contaminants in drinking water, and the SDWA requires that the EPA identify up to 30 additional unregulated contaminants for monitoring every 5 years.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/3881d73f4d4aaa0b85257359003f5348/9725165167f237b1852579f1007176e7!OpenDocument

[Return to top]

Public Health and Healthcare Sector

29. *May 3, Salt Lake Tribune* – (Utah) **Utah Health Dept chief: Hacked data stored too long.** Medical data hacked in March from a State of Utah computer server languished in the State's electronic system instead of being erased within a day, which is normal security protocol, the Utah Department of Health executive director said May 1. At a community forum held by the department, he said Social Security numbers and other personal information stayed on the poorly protected server for 3 months. The information, he said, "should have been deleted the day after the inquiry." By "inquiry," he meant the information routinely sent out by health care providers, as part of their billing, to check whether patients are covered by Medicaid. That means patient names, birth dates, and Social Security numbers go through the health department's computer system. He later stated the breach was not the fault of the providers. "They did not expect to see this [personal health information] saved on our server. The data should not have been there when it was compromised," he said.
Source: http://www.sltrib.com/sltrib/news/54037017-78/health-security-department-patton.html.csp

30. *May 2, Washington Times* – (National) **Medical professionals charged with fraud involving Medicare.** A strike force of federal, state, and local agents and investigators, led by the Departments of Justice and Health and Human Services, has charged 107 persons in 7 cities with Medicare fraud involving more than $452 million in false billings, the U.S. Attorney General said May 2. He described the sweep as the highest amount of apparent false Medicare billings involved in a single takedown in the 5-year history of the government's Medicare Fraud Strike Force. Those charged included doctors, nurses, social workers, health care company owners, and others — all accused of a range of serious offenses, including health care fraud, conspiracy to commit health care fraud, money laundering, and violation of laws against kickbacks. The arrests were made in Los Angeles, Chicago, Miami, Houston, Detroit, Baton Rouge, Louisiana, and Tampa, Florida. More than 500 agents and investigators took part in the operation.
Source: http://www.washingtontimes.com/news/2012/may/2/medical-professionals-charged-with-fraud-involving/

For another story, see item **36**

[Return to top]

Government Facilities Sector

31. *May 3, CNN* – (Tennessee) **Small explosion at Tennessee high school, 1 taken to hospital.** A pair of makeshift bombs blew up May 3 inside a Memphis, Tennessee high school, causing one person to be taken to a hospital, officials said. The "pressurized" devices, which incorporated Drano clog remover, were placed in different hallways — one on the second floor, the other on the third floor — of Craigmont High School, said a Memphis Fire Department official. "What it appears is that we had a student or two do a prank," said a spokeswoman for Memphis schools. An assistant principal sought medical treatment after inhaling smoke from one of the bombs while evacuating students. Memphis police and members of the federal Bureau of Alcohol, Tobacco, Firearms, and Explosives were also at the scene.
Source: http://www.cnn.com/2012/05/03/us/tennessee-school-blast/index.html?hpt=hp_t3

32. *May 2, WTOP 103.5 Washington, D.C.* – (Maryland) **Secret government records misplaced at National Archives.** The National Archives is taking action following an inspector general's (IG) report that found thousands of boxes of secret government records unaccounted for at its facility in Suitland, Maryland, WTOP 103.5 Washington, D.C. reported May 2. The report, first obtained through a Freedom of Information Act request from the Washington Times, found more than 2,300 boxes of classified files had gone missing from the Washington National Records Center. Since the report was issued in 2011, the Archives says it has accounted for about 640 missing boxes. It is still investigating the whereabouts of another 1,708. The IG report blames faulty data for the loss of the material. In the case of the 640 boxes that have been found, there were discrepancies between tracking numbers in the Archives' computerized database and the numbers on the boxes themselves. The executive for agency services at the National Archives says the agency is in the process of doing the research necessary to

clear discrepancies in the remaining 1,708 boxes. Most of the material is not thought to be missing from the facility itself.
Source: http://www.wtop.com/41/2850449/Secret-government-records-misplaced-at-National-Archives

33. *May 2, SecurityNewsDaily* – (National; International) **New 'Unknowns' hacking group hits NASA, Air Force, European Space Agency.** A new hacking group calling itself "The Unknowns" published May 1 a list of passwords and documents reportedly belonging to NASA, the European Space Agency, and the U.S. Air Force, among other high-profile government targets. The group's Pastebin post includes names and passwords reportedly belonging to NASA's Glenn Research Center as well as the U.S. Military's Joint Pathology Center, the Thai Royal Navy, Harvard University, Renault, the Jordanian Yellow Pages, and the Ministries of Defense of France and Bahrain. Softpedia reports the hackers also posted screenshots of some of the sites they breached, and that although the post was made public May 1, some of the hacks date back to March. In its message, The Unknowns explained the impetus for their exploits, and warned they could have defaced all of the Web sites. The hackers said they can provide information on how they penetrated the databases, and told the affected organizations to contact them.
Source: http://www.securitynewsdaily.com/1804-unknowns-hackers-nasa-air-force.html

34. *May 2, WFTV 9 Orlando* – (Florida) **DCF warns child care workers of possible computer security breach.** The Florida Department of Children and Families sent out letters to 100,000 child care workers statewide about a possible breach in security, WFTV 9 Orlando reported May 2. The employees' personal information, including dates of birth and Social Security numbers, was stored online and not password protected by a vendor. "During the time the information was unprotected, there was only legitimate uses for that information, only legitimate uses conducted by the vendor," said a department spokesperson.
Source: http://www.wftv.com/news/news/local/dcf-warns-child-care-workers-possible-computer-sec/nNPrz/

35. *May 2, Birmingham News* – (Alabama) **3 men charged with concealing, selling stolen Army telescopic rifle scopes.** May 2, a federal grand jury indicted three Birmingham, Alabama-area men on charges of concealing and selling stolen U.S. Army telescopic rifle scopes, federal officials announced. The indictment charges that between January 2010 and March 2010 the 3 men received and concealed 63 Aimpoint CompM2 optical rifle sights and two ACOG Model TA31RCO optical rifle sights they knew had been stolen from the Army. The Army paid $18,164 for the rifle sights. The indictment also charges that the three men conspired to conceal and sell the stolen rifle sights to a Hoover business. The business became suspicious of the sights, contacted authorities, and cooperated throughout the investigation.
Source: http://blog.al.com/spotnews/2012/05/3_men_charged_with_concealing.html

For more stories, see items **47** and **51**

[Return to top]

Emergency Services Sector

36. *May 2, Houston Chronicle* – (Texas) **Largest-ever medicare fraud takedown nabs 4 Houston EMS providers.** Nearly 100 suspects tied to more than $450 million in phony Medicare billings in Houston and six other cities were arrested May 2 in what is believed to be the largest health care fraud take-down in U.S. history. The arrests, made by investigators with the U.S. Department of Health and Human Services' Office of Inspector General and FBI agents, included operators of four Houston private ambulance companies responsible for $7 million in phony trips to an outpatient psychiatric clinic. The ambulance owners charged were accused of submitting claims that prosecutors said were not covered because patients were transported to a community mental health center (CMHC), not a hospital or medical facility. CMHCs are a Medicare-created entity that does not require a license in Texas. "Medicare did not cover ambulance transport from a beneficiary's home to a CMHC because a CMHC was not a hospital, skilled nursing facility or dialysis center," the indictments said.
Source: http://www.emsworld.com/news/10708720/largest-ever-medicare-fraud-takedown-nabs-4-houston-ems-providers

37. *May 1, Scripps Howard News Service* – (National) **Tasers can be tied to cardiac arrest and death, new study finds.** A new study published the week of April 30 in the journal Circulation finds the use of Tasers can be tied to cardiac arrest and death. The study represents the first peer-reviewed evidence that Tasers can bear a lethal risk. An electrophysiologist at Indiana University wrote that a review of "animal and clinical data" showed that Taser strikes to the chest can "cause cardiac electrical capture," which can trigger a heart attack. The Taser, used by about 16,000 law enforcement agencies around the world, is marketed as a way to subdue an individual without causing substantial injury or death, but since 2001, more than 500 people have died following Taser stuns, according to Amnesty International, which said in February that stricter guidelines for its use were "imperative." Although, in only a few dozen of those cases have medical examiners ruled the Taser contributed to the death. And TASER International, the company who makes the weapon, cited a U.S. Department of Justice study in May that concluded "there is currently no medical evidence that CEDs (controlled energy devices, which include Tasers) pose a significant risk." The Justice study also reported that "the risks of cardiac arrhythmias or death remain low and make CEDs more favorable than other weapons."
Source: http://www.therepublic.com/view/story/tasers-heart/tasers-heart/

For more stories, see items **4**, **26**, and **30**

[Return to top]

Information Technology Sector

38. *May 3, Help Net Security* – (International) **RedKit exploit kit spotted in the wild.** A new exploit kit Trustwave researchers spotted in the wild is aiming to enter a market

practically monopolized by the BlackHole and Phoenix exploit kits. This new kit has no official name, so the researchers dubbed it RedKit due to the red coloring scheme of its administration panel. RedKit's creators decided to promote it by using banners, and potential buyers are required to share their Jabber username by inputting it into an online form hosted on a compromised site of a Christian church. Equipped with this piece of data, the developers contact the buyers and provide them with a demo account so they can examine the software. The admin panel looks similar to other kits, and offers the usual tools: statistics for incoming traffic and the option to upload a payload executable and scan it with 37 different antivirus programs. As each malicious URL gets blocked by most security firms in the first 24 to 48 hours, the kit developers also provide an API that produces a fresh URL every hour, so customers can set up an automated process for updating traffic sources to point to the new URL. To deliver the malware, RedKit exploits two popular bugs: the Adobe Acrobat and Reader LibTIFF vulnerability (CVE-2010-0188) and the Java AtomicReferenceArray vulnerability (CVE-2012-0507), lately used by the criminals behind the massive Flashback infection.
Source: http://www.net-security.org/malware_news.php?id=2096&utm

39. *May 3, Help Net Security* – (International) **'Free additional storage' phishing emails doing rounds.** Symantec researchers warned about a variety of fake e-mails supposedly coming from popular e-mail and online storage services, offering "storage quota upgrades." A click on the offered link takes the potential victims to a bogus page mimicking the service's legitimate one. The page offers a variety of storage plans — from 20 GB to 1 TB — supposedly free of charge. "Your new plan will automatically renew each year, but you can disable auto-renewal at any time by returning to this page and choosing additional free plan," says the poorly worded offer. "We will contact you 30 days prior to renewal. Please allow up to 24 hours for your new storage amount to appear in all services," the scammers conclude, so that the users are not alarmed when they do not see an immediate change. In order to select one of the offered storage plans, users must input e-mail address (username) and password, which are promptly sent to the scammers. In the meantime, the users are redirected first to another bogus page notifying them of a successful storage quota upgrade, then to the service's legitimate Web sites.
Source: http://www.net-security.org/secworld.php?id=12858&utm

40. *May 3, Threatpost* – (International) **Serious remote PHP bug accidentally disclosed.** A serious remote-code execution vulnerability in PHP was accidentally disclosed May 2, leading to fears of an outbreak of attacks on sites built using vulnerable versions of PHP. The bug was known privately since January when a team of researchers used it in a game and then subsequently reported it to the PHP Group. The developers were still in the process of building the patch for the flaw when it was disclosed May 2. The vulnerability is simple, but it has serious consequences — the researchers found when they passed a specific query string containing the -s command to PHP in a CGI setup, PHP would interpret the -s as the command line argument and result in the disclosure of the source code for the application. They extended their testing and found they could pass whatever command-line arguments they wanted to the PHP binary. "A remote unauthenticated attacker could obtain sensitive information, cause a denial of service condition or may be able to execute arbitrary code with the

privileges of the web server," according to an advisory published May 2 by the U.S. Computer Emergency Readiness Team. The team that found the bug, Eindbazen, said they waited for several months for the PHP Group to release a patch for the vulnerability to publish information about it. However, someone accidentally marked an internal PHP bug as public and it was eventually posted online. As a result, Eindbazen published the details of their findings and how it can be exploited.
Source: http://threatpost.com/en_us/blogs/serious-remote-php-bug-accidentally-disclosed-050312

41. *May 3, Nextgov* – (International) **Companies increasingly are dissecting malware in the cloud.** Companies increasingly are looking at malware as a source of intelligence to learn more about the threats they face, Dark Reading reports. One of the ways to do this is by using products that provide malware analysis in the cloud. Companies that chance on suspected malware on their networks can upload it to an Internet — or cloud-based — service and get an automated report back detailing how malicious the worm is. These products help firms analyze how malware enters their systems if they do not have the expertise to do it on their own. Companies have historically tapped software or hired security consultants to carry out malware analysis. Of course, organizations concerned that others would gain sensitive information about their system vulnerabilities will have to do the analysis in-house, the report notes.
Source: http://www.nextgov.com/cloud-computing/2012/05/companies-increasingly-are-dissecting-malware-cloud/55559/

42. *May 3, Computerworld* – (International) **Microsoft plans big May patch slate for next week.** May 3, Microsoft said it would ship 7 security updates the week of May 7 to patch 23 bugs in Windows, Office, and its Silverlight and .Net development platforms. Of the seven updates, Microsoft tagged three as "critical," and the other four as "important." Four updates will address vulnerabilities in Windows; four will impact Office; and one will affect the Silverlight development framework. That count exceeds seven because one of the updates tackles bugs in all three of those lines.
Source:
http://www.computerworld.com/s/article/9226846/Microsoft_plans_big_May_patch_slate_for_next_week?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Re

43. *May 2, Krebs on Security* – (International) **OpenX promises fix for rogue ads bug.** Hackers are actively exploiting a dangerous security vulnerability in OpenX — an online ad-serving solution for Web sites — to run booby-trapped ads that serve malware and browser exploits across countless Web sites that depend on the solution. For months, security experts have been warning about mysterious attacks on OpenX installations in which the site owners discovered new rogue administrator accounts. That access allows miscreants to load tainted ads on sites that rely on the software. The bad ads usually try to foist malware on visitors, or frighten them into paying for bogus security software. OpenX is only now just starting to acknowledge the attacks, as more users are coming forward with unanswered questions about the mysteriously added

administrator accounts.
Source: http://krebsonsecurity.com/2012/05/openx-promises-fix-for-rogue-ads-bug/

44. *May 2, ZDNet* – (International) **A first: Hacked sites with Android drive-by download malware.** Cyber criminals often put drive-by download malware on Web sites they have hacked in order to quickly infect visitors' PCs. For the first time though, hacked Web sites with Android drive-by download malware were discovered. A new trojan, called NotCompatible, appears to serve as a simple TCP relay while posing as a system update named "Update.apk." It does not currently appear to cause any direct harm to a target Android device, but could potentially be used to gain access to private networks by turning an infected smartphone into a proxy. IT administrators should note a device infected with NotCompatible could potentially be used to infiltrate normally protected information or systems, such as those maintained by enterprises or governments. The device needs to be set to approve applications not from the Google Play store, and the user has to agree to install the app.
Source: http://www.zdnet.com/blog/security/a-first-hacked-sites-with-android-drive-by-download-malware/11810

For more stories, see items **5**, **29**, **33**, and **34**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

45. *May 2, Lake County News* – (California) **KPFZ off air temporarily due to technical difficulties.** Lake County Community Radio KPFZ 88.1 FM in Lakeport, California, went offline for unknown reasons May 2. The station's manager identified the problems and got the station back on the air at approximately 3:30 p.m. Earlier in the day, the issue was believed to be related to the transmitter site on Buckingham Peak, but it was later found to be a localized issue that was resolved. The station went off the air around 11:30 a.m.
Source:
http://www.lakeconews.com/index.php?option=com_content&view=article&id=24842:kpfz-off-air-temporarily-due-to-technical-difficulties&catid=1:latest&Itemid=197

46. *May 2, KSEE 24 Fresno* – (California) **AT&T's service suffers from copper thefts in Fresno.** AT&T's communications in California are being cut by copper wire thieves and the Fresno County Sheriff's department and AT&T are teaming up to catch those responsible. The latest copper theft happened May 2. Two severed wires were dangling from the lines; AT&T said 300-feet were missing. Lincoln Avenue was targeted six

times. Earlier in 2012, the county began cementing copper telephone boxes in the ground, but the countermeasure has thieves reaching to new heights for the metal. The theft has cost AT&T thousands, and Fresno County has spent over a half a million dollars in 2012 alone. Recently, in Madera, a copper thief cut one pole down and it had a domino effect, bringing eight telephone poles down along with it. There were 30 attacks in Fresno and Madera in the past 2 months; thousands of customers were affected.
Source: http://www.ksee24.com/news/local/ATT-Crime---CLU-149924075.html

For another story, see item **44**

[Return to top]

Commercial Facilities Sector

47. *May 3, Associated Press* – (Wisconsin) **Strong storms cause flooding, damage in Wisconsin.** Strong thunderstorms knocked down trees and power lines, and caused hail damage to homes and businesses in Wisconsin, May 2. In Manitowoc County, access to the Town of Rockwood was closed because of high flood waters. Flooding also closed a portion of Highway 41 in both directions in Winnebago and Fond du Loc counties. The Blair-Taylor school district called off classes May 3 because of storm damage. Numerous power lines and trees were down. About 30 homes in the Arcadia trailer park sustained wind and hail damage. Wisconsin Public Service said the storms interrupted power for about 3,000 customers in Rhinelander, Green Bay, and Tomahawk.
Source:
http://www.wausaudailyherald.com/article/20120503/WDH0101/120503010/Hail-damages-down-power-lines-reported-from-overnight-storm-western-Wis-?odyssey=mod|mostview

48. *May 2, Wyckoff-Franklin Lakes Patch* – (New Jersey) **Carbon monoxide forces evacuation of Boulder Run apartments, stores.** Dangerously high carbon monoxide levels at the Boulder Run apartments and shops in Wyckoff, New Jersey, forced residents, employees, and customers in one section of the strip mall to be evacuated May 2. Firefighters donned breathing masks and entered the apartments to evacuate residents. According to the Wyckoff Fire Department chief, someone in a non-operational storefront on the ground floor was using a concrete saw that caused carbon monoxide levels to rise to about 180 parts per million in the residence above. He added that the type of saw believed to have caused the incident should not be used in a closed environment. Residents were allowed to return after about 2 hours.
Source: http://wyckoff.patch.com/articles/carbon-monoxide-leak-forces-evacuation-of-boulder-run-apartments-stores

49. *May 2, WXIN 59 Indianapolis* – (Indiana) **State adopts new rules for outdoor stages at fairs and festivals.** The Indiana Fire Prevention and Building Safety Commission adopted new regulations May 2 regarding the construction and inspection of temporary stages at State and county fairs and festivals. The rules require any structure, like a

stage with overhanging equipment and lights, would need to be designed by licensed professionals and engineers and inspected by the State fire marshal's office or local authorities. The changes come in the wake of 2011's Indiana State Fair tragedy when seven people were killed and dozens injured by the collapse of the stage for the group Sugarland's concert. An investigation revealed high winds overcame the stage roof's rigging configuration. Audience members were also not evacuated in a timely manner.
Source: http://www.fox59.com/news/wxin-new-rules-state-fairs-state-adopts-new-rules-for-outdoor-stages-at-fairs-and-festivals-20120502,0,7815909.column?track=rss

50. *May 2, WHIO 7 Dayton* – (Ohio) **Suspected meth lab found at Butler Twp. motel.** Police looking for a wanted suspect at a motel in Butler Township, Ohio, May 2, instead discovered a meth lab that a man said he had set up in his room. Police were dispatched to the motel after people called the department because they thought they had seen a man who was wanted by police. When police arrived at the motel and knocked on the door, a different man answered and the officers said they noticed a chemical odor. The man told police that he had a meth lab in his room. Police then removed him from his room and evacuated the first three floors of the hotel while a HAZMAT team handled the chemicals inside.
Source: http://www.whiotv.com/news/news/suspected-meth-lab-found-butler-twp/nNPrZ/

51. *May 2, Associated Press* – (California) **Irvine homes, high school evacuated for gas leak.** Fire officials in Irvine, California, evacuated a high school and about 100 homes and apartments after construction crews struck and ruptured a natural gas line, May 2. An Orange County Fire Authority spokesman said Northwood High School was immediately evacuated because it was downwind of the leak. Gas company workers were working to stop the leak, and people within a half-mile perimeter were also evacuated as a precaution. The spokesman said that Portola Parkway was completely shut down for several hours as workers stopped the leak.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/05/02/state/n151706D29.DTL

For more stories, see items **1**, **24**, and **52**

[Return to top]

National Monuments and Icons Sector

52. *May 3, Associated Press* – (Texas) **Forest Service: West Texas Blazes nearly contained.** Firefighters made good progress controlling a pair of wildfires that torched about 24,000 acres close to a small residential community in Fort Davis, Texas. A Texas Forest Service spokeswoman said the Spring Mountain fire was about 60 percent contained. An evacuation order was issued the week of April 30 at the Davis Mountain Resort after that fire blew to within half a mile of the development. A larger blaze at the Livermore Ranch was deemed in "good shape," and nearly contained by fire lines. The spokeswoman said firefighters hoped to complete the fire containment lines on that blaze May 3. No building damage or injuries were reported from the fires.

Source: http://www.firehouse.com/news/10709107/forest-service-west-texas-blazes-nearly-contained

53. *May 2, Arizona Republic* – (Arizona) **Crews fight 40-acre wildfire outside Superior.** U.S. Forest Service officials said crews were battling a 40-acre fire near Superior, Arizona, in the Tonto National Forest, located about 70 miles east of central Phoenix. The Telegraph Fire was reported May 2 on Telegraph Mountain and burned 3 miles south of Picketpost Mountain outside Superior, according to a Tonto National Forest spokesman. The fire was estimated at 40 acres and access to the area was difficult, he said. About 50 personnel, including crews from Payson and Globe, were battling the flames, and air tankers made several retardant drops. Forest officials said one attack plane, three single-engine air tankers, and three heavy air tankers responded. An additional helicopter was also expected to assist. The cause of the fire remained under investigation and no properties were threatened.
Source: http://tucsoncitizen.com/arizona-news/2012/05/02/crews-fight-40-acre-wildfire-outside-superior/

[Return to top]

Dams Sector

Nothing to report

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2314
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer